WEB SECURITY ASSESSMENT REPORT

Target

demo.testfire.net

Assessment Type

Passive Security Review

Presented by

Anshika Singh

Date: 08/02/2026

WEB APPLICATION SECURITY ASSESSMENNT REPORT

This report presents the results of a passive web application security assessment conducted on the publicly accessible website demo.testfire.net. The purpose of this assessment is to identify common security configuration weaknesses and assess the overall security posture of the application using non-intrusive methods.

The assessment was performed as a read-only review, focusing on observable security controls such as HTTP response headers, server information disclosure, and cookie configuration. No exploitation, authentication testing, or intrusive techniques were used at any stage of the assessment.

This report has been prepared for educational purposes and demonstrates a structured approach to web security assessments aligned with industry best practices, including guidance from the Open Web Application Security Project (OWASP).

The findings documented in this report include identified security weaknesses, associated risk levels, and recommended remediation actions. In addition, positive security controls observed during testing are also highlighted to provide a balanced and accurate assessment.

Target Website: demo.testfire.net
Assessment Type: Passive / Read-Only Security Review
Prepared by: Anshika Singh
Date: 08 February 2026

SCOPE & METHODOLOGY

Scope

The scope of this security assessment was limited strictly to publicly accessible components of the target web application. Only unauthenticated pages were reviewed, and no login functionality or user-specific features were tested. The assessment did not include any form of exploitation, vulnerability scanning that could impact availability, or attempts to bypass security controls.

The review focused on identifying configuration-related security issues that are visible through passive observation. This included the analysis of HTTP response headers, cookie attributes, and information disclosed through server responses.

Methodology

The assessment was conducted using passive, read-only techniques to ensure no impact on the target system. Browser Developer Tools were used to inspect network traffic, HTTP headers, and cookies generated during normal page loads. All observations were made without modifying requests or injecting malicious input.

The findings were evaluated against widely accepted security best practices, including OWASP recommendations for secure web application configuration. This approach ensures the assessment remains ethical, accurate, and suitable for educational demonstration purposes.

EXECUTIVE SUMMARY

A passive security assessment was conducted on the target web application to evaluate its security configuration and identify potential weaknesses that could increase exposure to common web-based threats. The assessment was limited to non-intrusive testing methods and focused on observable behaviors during normal application usage.

The review identified a total of three notable observations. One medium-risk security issue was identified relating to missing HTTP security headers, which may increase the application's exposure to certain client-side attacks. In addition, one low-risk issue involving server version disclosure was observed. While this issue does not pose an immediate threat, it may assist attackers during reconnaissance activities.

The assessment also identified a positive security control. Session cookies were found to be configured with appropriate security flags, demonstrating adherence to secure session management best practices.

No critical or high-risk vulnerabilities were identified during the assessment. Overall, the application demonstrates partial implementation of security best practices, with opportunities for improvement through standard configuration hardening.

Overall Risk Rating: Medium

The implementation of recommended security headers would significantly improve the application's overall security posture.

FINDING OVERVIEW

This section provides a high-level summary of the findings identified during the security assessment. Each finding has been categorized based on its potential impact and likelihood, using qualitative risk ratings of Medium, Low, or Positive Observation.
The findings primarily relate to configuration-level security controls rather than exploitable application flaws. This is consistent with the passive and read-only nature of the assessment.
The table below summarizes the identified findings:

- *Missing Security Headers (Medium Risk): Several recommended HTTP security headers were not implemented, increasing exposure to client-side attacks.*
- *Server Version Disclosure (Low Risk): The server response includes backend technology information that could assist attackers during reconnaissance.*
- *Secure Cookie Configuration (Positive Finding): Session cookies were observed to include appropriate security flags, reducing the risk of session compromise.*

This overview allows stakeholders to quickly understand the overall security posture before reviewing the detailed findings in subsequent sections. Detailed descriptions, evidence, and remediation recommendations for each item are provided in the following pages.

FINDING 1: Missing Security Headers

Description

The assessment identified that the web application does not implement several recommended HTTP security headers. These headers are designed to provide additional layers of protection against common client-side attacks.

Observed Missing Headers

- *Content-Security-Policy*
- *X-Frame-Options*
- *Referrer-Policy*

Risk:

The absence of these security headers increases the likelihood of client-side attacks such as cross-site scripting (XSS) and clickjacking. Without these protections, an attacker may be able to execute malicious scripts in a user's browser or embed the application within a malicious frame.

Severity: *Medium*

Recommendation

It is recommended that the application implements standard HTTP security headers in accordance with OWASP guidelines. Proper configuration of these headers can significantly reduce the risk of client-side exploitation and improve overall security posture.

Evidence for this finding was obtained through inspection of HTTP response headers using browser developer tools.

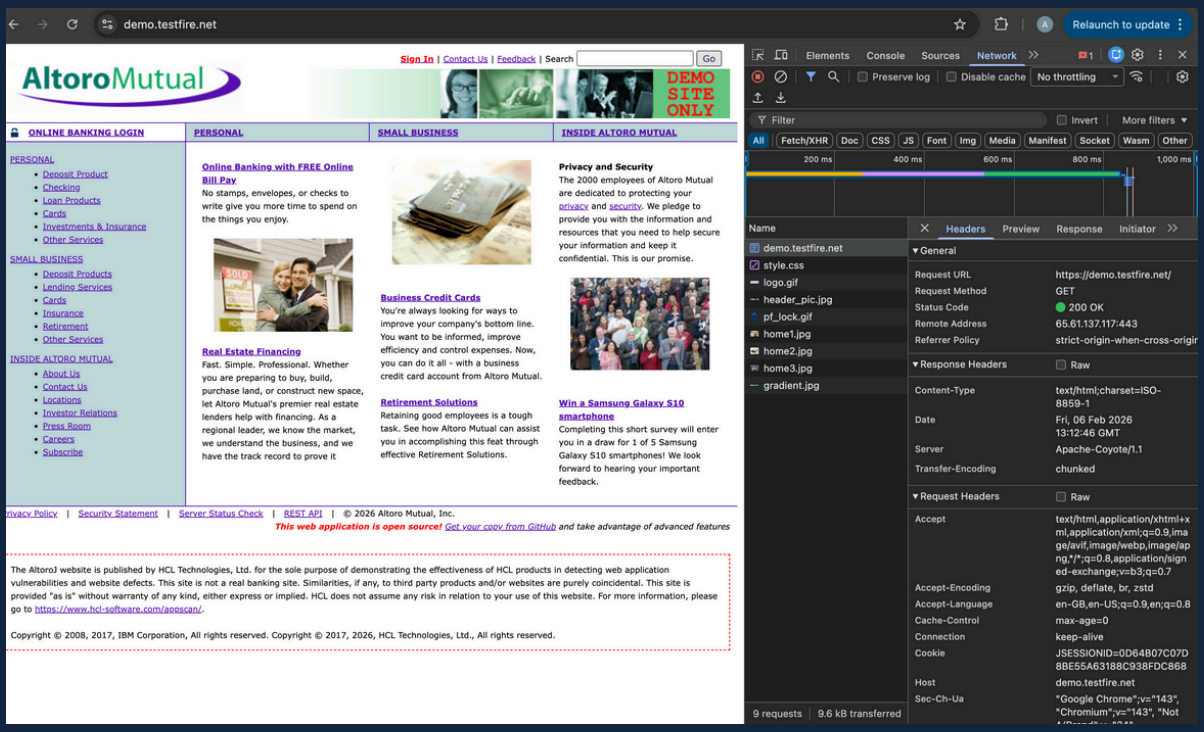

Figure 1: illustrates the HTTP response headers returned by the application. The server discloses its backend technology through the Server header, which reveals Apache-Coyote/1.1. Additionally, several recommended security headers (such as Content Security Policy, X-Frame-Options, and X-Content-Type-Options) are not present in the response. Disclosure of server details and missing security headers can increase the application's attack surface by providing useful information to attackers and reducing protection against common web-based attacks.

FINDING 2: Server Version Disclosure

Description

The assessment identified that the web server includes version information within the HTTP response headers. Specifically, the server header discloses details about the underlying server technology.

Evidence

The following header was observed during testing:
Server: Apache-Coyote/1.1

Risk

While server version disclosure does not directly expose the application to exploitation, it may assist attackers during reconnaissance and profiling activities. Knowledge of backend technologies can help attackers tailor attacks to known vulnerabilities associated with specific software versions.
Severity: Low

Recommendation

It is recommended that server version information be removed or obfuscated where possible. This can typically be achieved through server configuration changes and helps reduce unnecessary information disclosure to external users

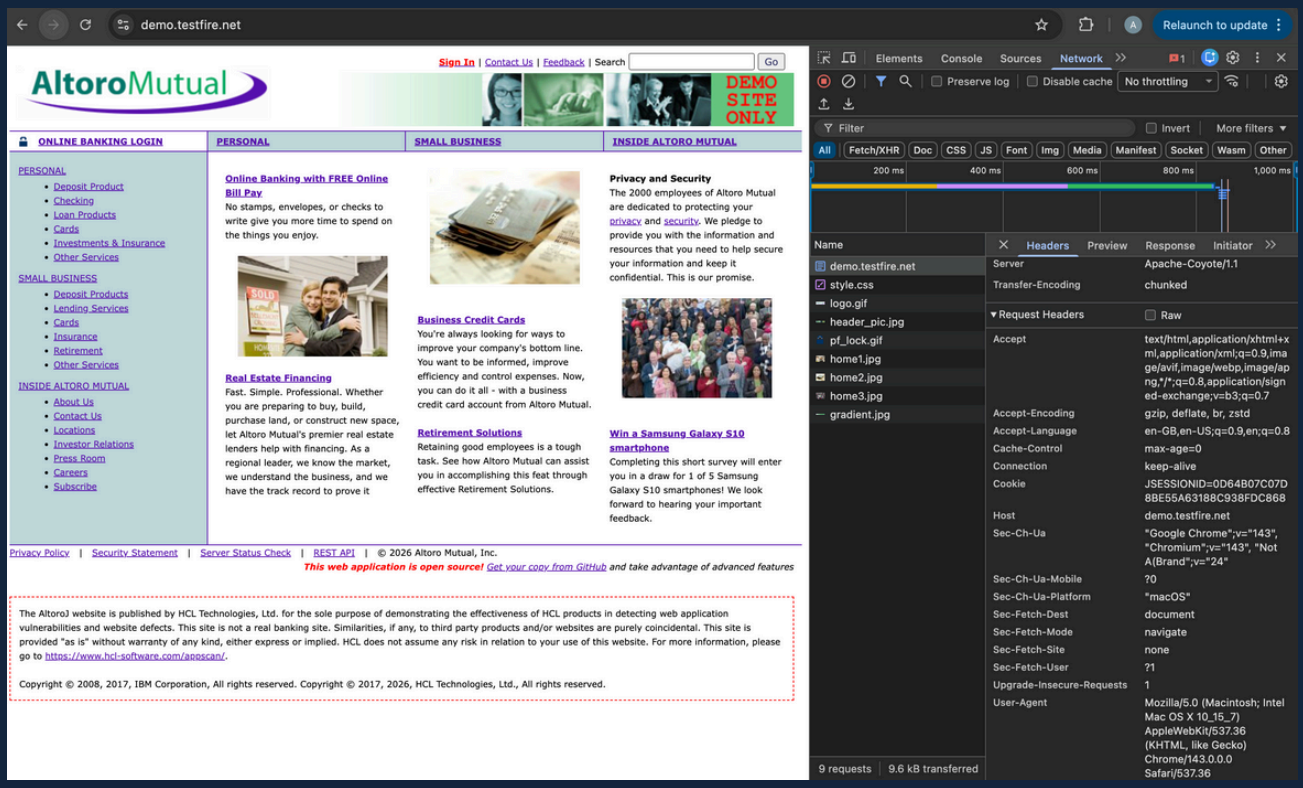

Figure 2 shows the HTTP response headers captured during the assessment. The application discloses backend server information through the Server header, which reveals Apache-Coyote/1.1. Exposing server version details can assist attackers in identifying known vulnerabilities associated with the underlying technology. This finding indicates unnecessary information disclosure and highlights the need to limit server-related header information.

POSITIVE FINDING: Secure Cookie Configuration

Description

During the assessment, session cookies were reviewed to evaluate their security configuration. The cookies were observed to include appropriate security attributes.

Observed Controls

- ***Secure flag enabled***
- ***HttpOnly flag enabled***

Security Benefit

The Secure flag ensures that cookies are only transmitted over encrypted connections, reducing the risk of interception. The HttpOnly flag prevents client-side scripts from accessing cookie values, mitigating the risk of session theft through cross-site scripting attacks.

Assessment

This configuration demonstrates adherence to secure session management best practices and represents a positive security control within the application. While other areas require improvement, the proper handling of session cookies reduces the likelihood of session-based attacks.

This positive finding highlights the importance of recognizing existing security measures alongside identified weaknesses, providing a balanced and accurate assessment.

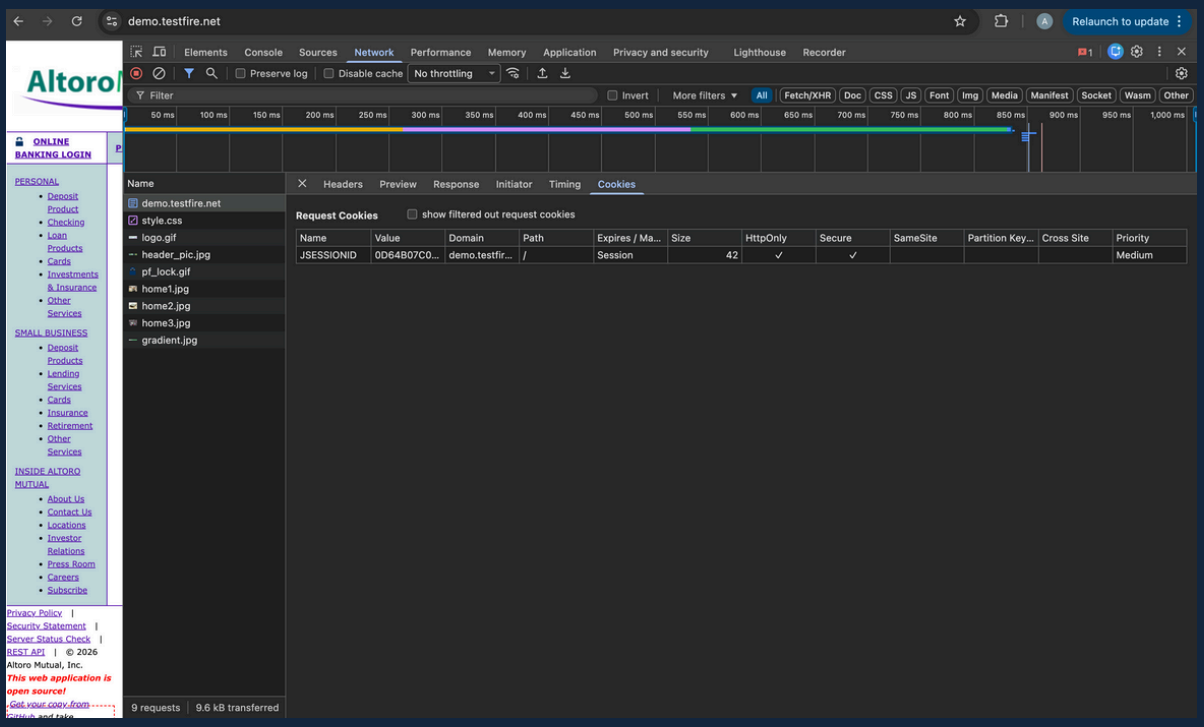

Figure 3: shows the session cookie configuration observed during the assessment. The JSESSIONID cookie is configured with both the Secure and HttpOnly flags enabled. The Secure flag ensures that the cookie is only transmitted over secure connections, while the HttpOnly flag prevents client-side scripts from accessing the cookie value. This configuration reduces the risk of session hijacking and demonstrates adherence to recommended session management best practices.

CONCLUSION

The passive security assessment identified several configuration-related security observations within the target web application. The most significant issue relates to missing HTTP security headers, which presents a medium-level risk and should be addressed to reduce exposure to client-side attacks.

A low-risk issue involving server version disclosure was also identified. While not critical, addressing this issue would further limit the information available to potential attackers during reconnaissance activities.

In contrast, the application demonstrates good practice in the configuration of session cookies. The presence of Secure and HttpOnly flags indicates partial adherence to security best practices and contributes positively to the application's overall security posture.

No critical vulnerabilities were identified during the assessment, and no exploitation was performed. Implementing the recommended configuration changes would significantly improve the security posture of the application with minimal effort.

DISCLAIMER

This security assessment was conducted using passive, read-only techniques and was limited to publicly accessible resources. No authentication testing, exploitation attempts, or intrusive techniques were performed at any time during the assessment.

The findings documented in this report reflect the security posture observed at the time of testing and may change as the application or its configuration evolves. This report does not guarantee the absence of vulnerabilities and should not be interpreted as a comprehensive security audit.

The assessment was performed for educational purposes only and is intended to demonstrate a structured approach to identifying common web application security configuration issues in an ethical and responsible manner.